Cyberbezpieczny Samorząd w Gminie Gilowice

Gmina Gilowice zrealizowała projekt dofinansowany z Funduszy Europejskich **„Cyberbezpieczny Samorząd w Gminie Gilowice”.**

Realizacja projektu była odpowiedzią na potrzeby wynikające z diagnozy, dotyczącej wzmocnienia zdolności do skutecznego zapobiegania incydentom bezpieczeństwa teleinformatycznego, wykrywania ich i reagowania na nie w Urzędzie Gminy Gilowice.

„**Cyberbezpieczny Samorząd w Gminie Gilowice”**

Program **Fundusze Europejskie na Rozwój Cyfrowy (FERC)**

Priorytet **II Zaawansowane usługi cyfrowe**

Działanie **2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa**

Wartość projektu ogółem**: 415 860,00 zł,**

Dofinansowanie **415 860,00 zł,** w tym:

dofinansowanie z Unii Europejskiej**: 341 005,28 zł**

dofinansowanie z Budżetu Państwa**: 74 854,72 zł**

Cały zakres inwestycji dotyczył Urzędu Gminy Gilowice.

- Celem projektu było zwiększenie poziomu bezpieczeństwa informacji poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych państwa oraz podmiotów mających kluczowe znaczenie dla gospodarki, zgodnie z polityką bezpieczeństwa UE i wytycznych Agencji UE ds. cyberbezpieczeństwa, koncentrując się na zbudowaniu zdolności reagowania na cyberataki.

Cel i zaplanowane efekty projektu były zgodne z celami FERC 2021-2027 Działanie 2.2

- Projekt realizował założenia AIP, zwłaszcza pryncypia zawarte w dokumencie z dn. 25 listopada 2020 r. i Deklaracji tallińskiej, w tym domyślności cyfrowej, jednorazowości, powszechności, dostępności, otwartości, przejrzystości, domyślnej transgraniczności i interoperacyjności oraz niezawodności i bezpieczeństwa. Projekt zapewniał również zgodność z zasadami równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn.

Zakres rzeczowy projektu obejmował trzy obszary: techniczny, kompetencyjny i organizacyjny.

1) **Obszar techniczny:** zadanie obejmowało modernizację infrastruktury IT, w tym: zakupiono serwer oraz zasilacze awaryjne UPS dla stacji komputerowych, jak również rozbudowano system backup RDX, system UTM, system DLP oraz system ochrony urządzeń. W obszarze wdrożono systemy informatyczne oraz testy penetracyjne.
2) **Obszar kompetencyjny:** zadanie obejmowało szkolenia kadr w zakresie cyberbezpieczeństwa.
3) **Obszar organizacyjny:** zadanie obejmowało m.in. audyt bezpieczeństwa, aktualizację dokumentacji, usługi doradcze, w tym opracowanie koncepcji cyfryzacji JST oraz usługi wsparcia na etapie realizacji projektu.